

MANRS Update for JET



Andrew Gallo
agallo@gwu.edu
Amreesh Phokeer
phokeer@isoc.org

Work streams

1. Ambassadors and mentors program
2. MANRS-sponsored academic research
3. MANRS Observatory improvements
4. Routing Security Summit 2023 – Research Roundup

<https://www.youtube.com/playlist?list=PL-p9v0NMIDhJv8QzdfBebHzK2BBUcyYza>



MANRS Ambassadors program



2023 Cohort

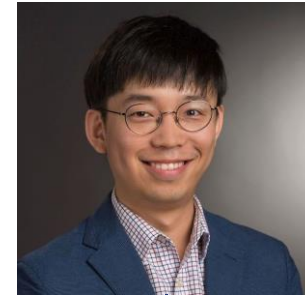
Project 1: Implementation of the MANRS+ tool (Jediel)

Project 2: DFOH and ASPA (Thomas)
(Detect Forged-Origin Hijacks)

Project 3: SAV tools and techniques (Nicolas)

Mentor

Tijay Chung (US)
Virginia Tech



Jediell Adefoulou
(Benin)



Thomas Holterbach
(France)



Nicolas Boettcher
(Chile)

Ambassadors



MANRS+

Initial MANRS program for network operators is a floor

ALL operators should *already* be implementing MANRS actions

MANRS+ is an enhanced, membership (and likely fee-based) program that will be more intensive. Exploring quality mark/trade mark/certification

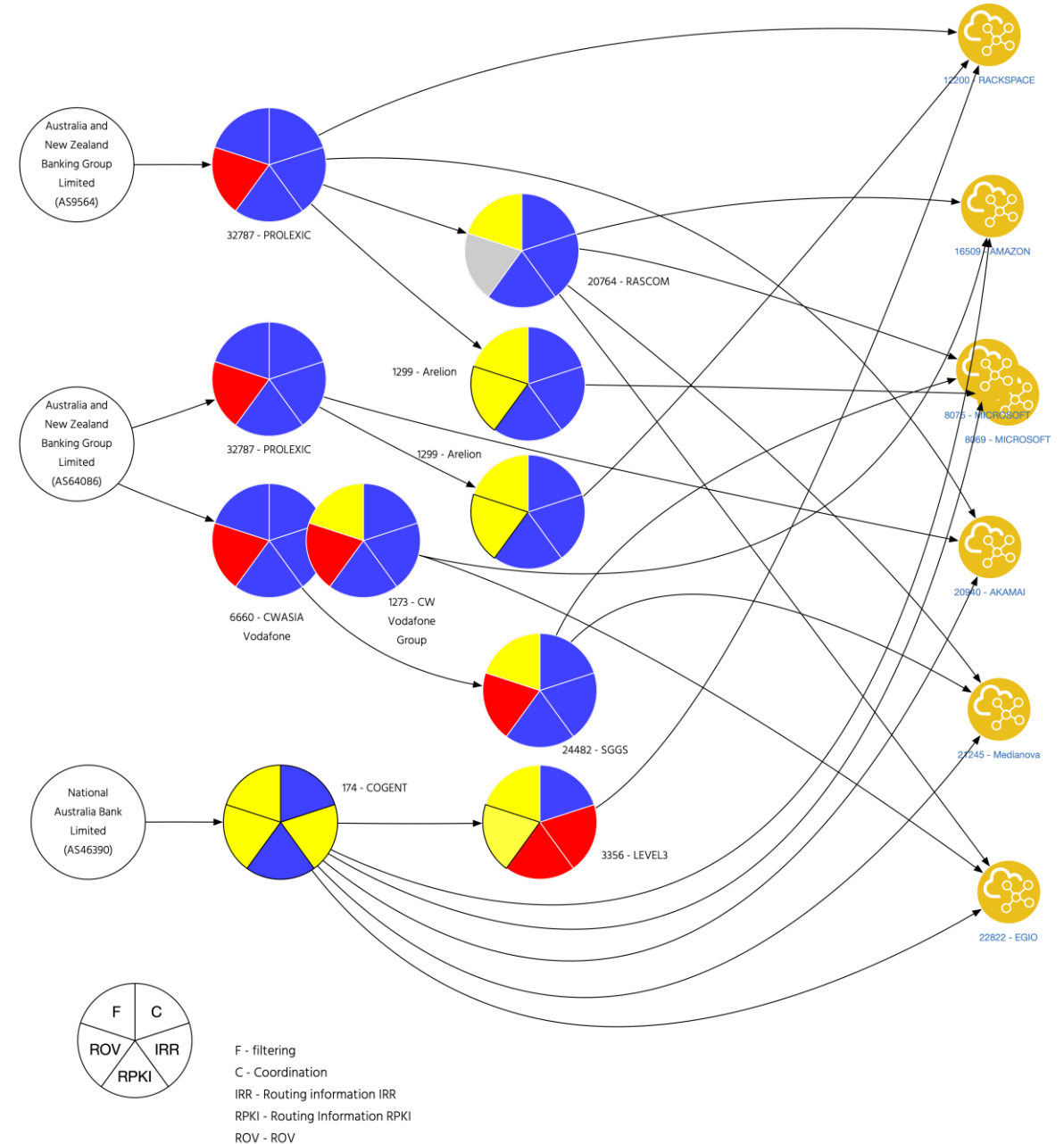
Routing Security is part of a broader supply chain security.

An internationally recognized authority is beneficial for procurement decision makers



MANRS+ tool

- Aim: to evaluate the risk factor of your supply chain (upstream providers and peers)
- Check the level of compliance



DFOH and ASPA

- **DFOH website** <http://dfoh.info.ucl.ac.be/>
Develop a website where operators and researchers can see the suspicious cases detected by DFOH in real time.
- **Longitudinal study**
Profiling the serial hijackers, pinpointing the suspicious cases that diverted traffic and caused traffic loss.
- **ASPA deployment**
Find a methodology to measure the adoption of ASPA by network operators



SAV tools and techniques

- ***SAV measurement survey***
A survey of existing SAV tools and techniques.
- ***Tools benchmarking***
Compare and contrast tools for SAV detection with CAIDA Spoofer
- ***Data gaps***
Identify CAIDA Spoofer data gaps



2022 Cohort

Project 1: RPKI Time measurement (Romain)

Project 2: Relying Party validation time (Zubair)

Project 3: ROVISTA (Tijay)

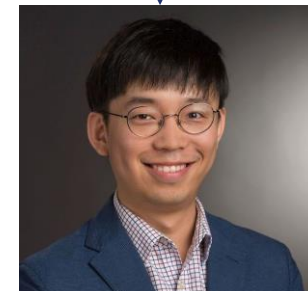
Project 4: RTBH and RPKI (Ioana)

Romain
Fontugne(JP)
IIJ

Massimo
Candela(NL)
NTT



Ioana Livadariu
(Norway)



Tijay Chung
(US)

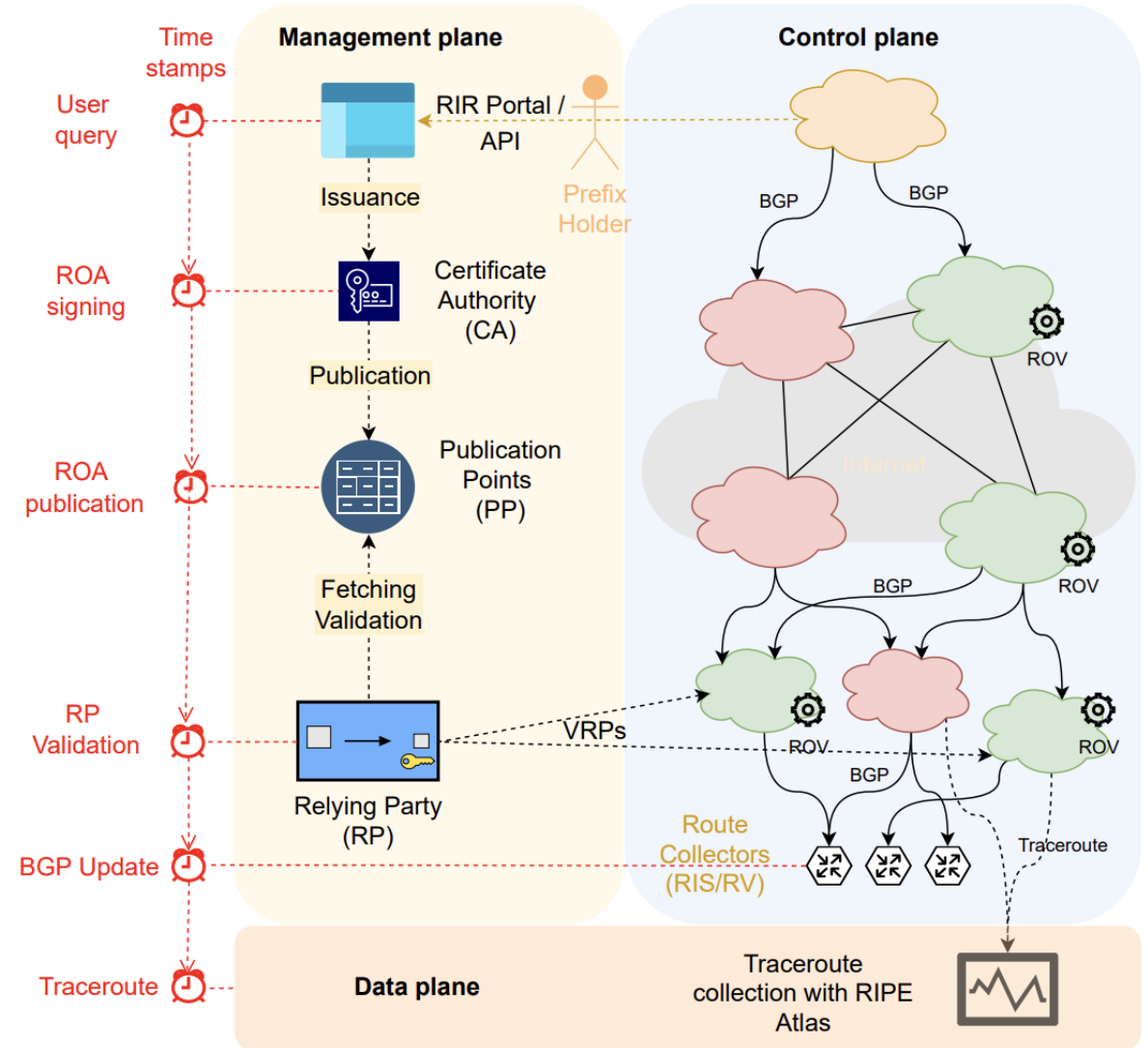


Zubair Sediqi
(Germany)



RPKI Time Measurement (PAM 2023)

- Each of the Five RIRs loaned us a set of IPv4 /24s and IPv6 /48s
- Prefixes were announced from one AS with ROV upstreams and some direct IX peers which were non-ROV
- Another set of RIPE prefixes from 3 ASs fed by non-ROV upstreams
- Measurements taken over eleven months



RPKI Time Measurement (PAM'23)

	Sign*	NotBefore*	Publication†	Relying Party†	BGP‡
AFRINIC	0 (0)	0 (0)	3 (2)	14 (13)	15 (16)
APNIC	10 (13)	10 (13)	14 (16)	34 (38)	26 (28)
ARIN	- (-)	- (-)	69 (97)	81 (109)	95 (143)
LACNIC	0 (0)	- (-)	54 (32)	66 (42)	51 (34)
RIPE	0 (0)	0 (0)	4 (4)	14 (13)	18 (18)
After fix:					
ARIN	- (-)	- (-)	8 (9)	21 (22)	28 (23)

	Revocation*	Relying Party†	BGP‡
AFRINIC	0 (0)	13 (14)	34 (38)
APNIC	10 (12)	31 (36)	51 (56)
ARIN	0 (0)	14 (16)	45 (51)
LACNIC	0 (0)	18 (20)	48 (49)
RIPE	0 (0)	14 (13)	41 (50)

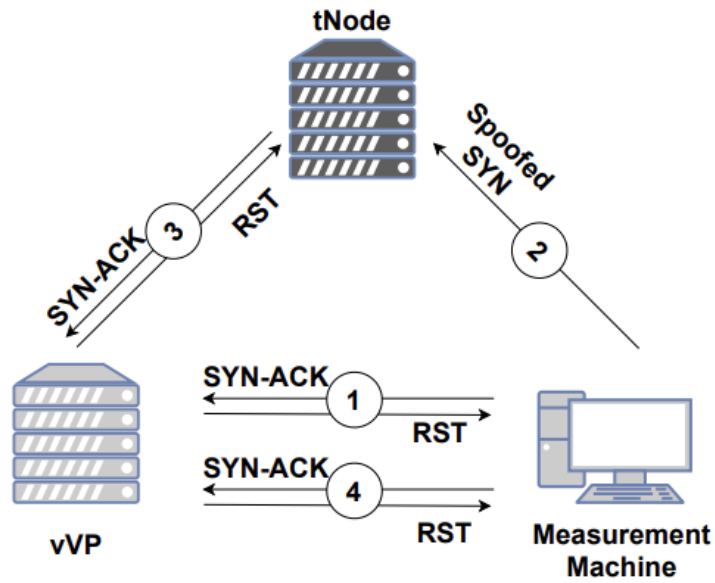


ROVISTA (Accepted at IMC'23)

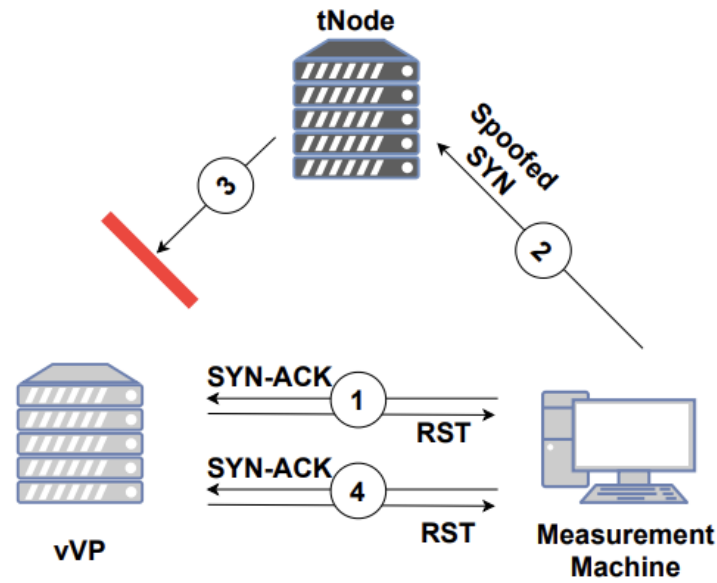
- Aim: an alternative way to measure the status of ROV in the wild
 - IPID side-channel (technique used to detect censorship)
- Current approaches have some limitations (coverage, active measurements)
 - Passive measurements (only BGP data)
 - RIPE Atlas has only 3700+ ASNs for IPv4 space
 - ROVISTA managed to get 27k ASNs
- Findings:
 - (44%) 12K ASNs not performing ROV
 - (9.4%) 2.6K ASNs are protected by ROV



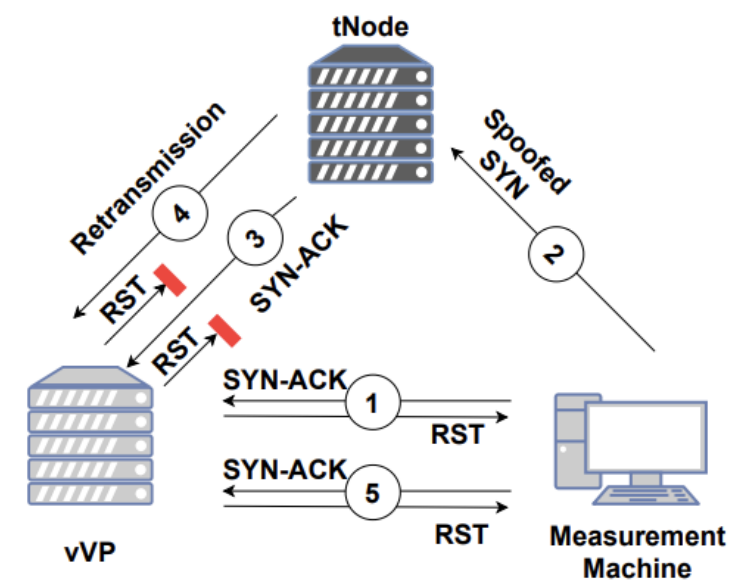
IP-ID side channel



(a) No filtering



(b) Inbound filtering



(c) Outbound filtering

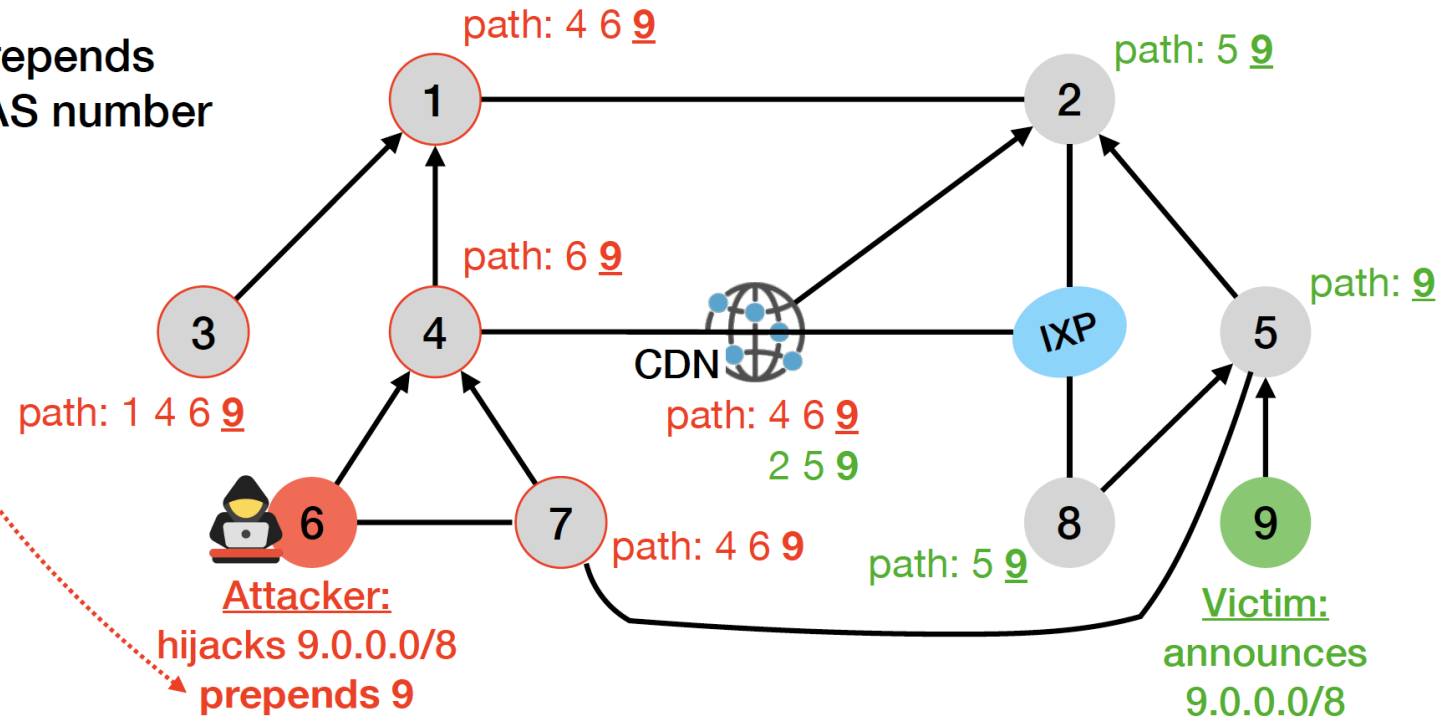


MANRS-sponsored academic research



Forged-origin hijacks

The attacker prepends the legitimate AS number to the AS path



Forged-origin hijacks

The Record.
Recorded Future® News

February 3, 2022

KlaySwap crypto users lose funds after BGP hijack


Hackers have stolen roughly \$1.9 million from South Korean cryptocurrency platform **KLAYswap** after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

The BGP hijack—which is the equivalent of hackers hijacking internet routes to bring users on malicious sites instead of legitimate ones—hit **KakaoTalk**, an instant messaging platform popular in South Korea.

The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has **confirmed** the incident last week and is currently **issuing compensation** for affected users.

August 17, 2022

 **CelerNetwork**
@CelerNetwork · [Follow](#)

 We are seeing reports that reflects potential DNS hijacking of cbridge frontend. We are investigating at the moment and please do not use the frontend for bridging at the moment.

11:56 PM · Aug 17, 2022

 321  Reply  Copy link

[Read 40 replies](#)



Detecting Forged Origin Hijacks (DFOH)

Protocol extensions

RPKI + ROV
BGPSec, ASPA

RPKI+ROV can't detect forged-origin hijacks
ASPA will take years to be deployed

Configuration guidelines

Route filters

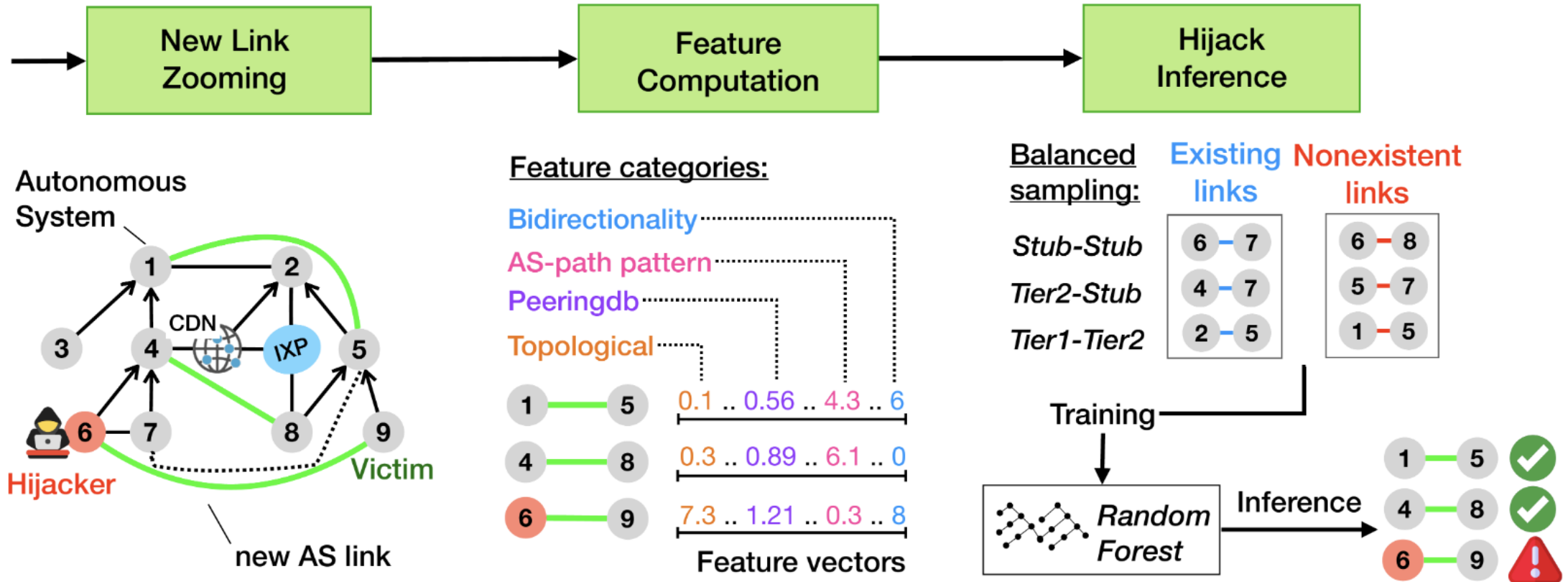
Often missing and inaccurate
as they are constructed based on the IRR

Monitoring platforms

ARTEMIS
BGPAlerter

Narrowly focused as they detect hijacks
that only pertain to the AS deploying it

DFOH under the hood



MANRS Observatory improvements



Improvements

- Finding an alternative data source to GRIP
 - Cloudflare Radar
 - Cachepoint
- Investigating technical solutions to reduce/eliminate bogons
- A few internal tools:
 - ROA History API
 - ROA-stats



Thank you.

agallo@gwu.edu

manrs.org



"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development
(NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674,
Fax: 202-459-9673, Email: nco@nitrd.gov, Website: <https://www.nitrd.gov>

